Amendments to the Claims:

1-20. (Canceled)

21. (New) A browser interface system for protecting a computer network, comprising:

a browser module that provides communications access to an unprotected network from a protected network, wherein said browser module is separate and physically distinct from protected computers;

a browser client module that communicates with the browser module, wherein said browser client module provides control of video and audio output of a browser operating remotely on said browser module; and

a browser isolator module that analyzes communications between the browser module and the browser client module,

wherein said browser isolator module prevents unauthorized communications between the browser module and the browser client module.

22. (New) The system of claim 21, wherein the communication between the browser module and the browser client module is limited to those communications specifically necessary for remote operation of the browser module.

23. (New) The system of claim 22, wherein the browser isolator module screens at least one of the following types of information to determine if the communication is authorized:

source and destination ports, user information, origination information, host information, destination information, character information, IP address information, display identification, session information, display class, display number, TCP information, and date and/or time information.

24. (New) The system of claim 21, wherein the browser module comprises a distributed network browser.

25. (New) The system of claim 21, wherein the protected network is isolated from unauthorized communications received from the unprotected network.

26. (New) The system of claim 21, wherein any browser-executed code operates on the browser module.

27. (New) The system of claim 21, wherein said browser isolator module prevents the transfer of permanently stored data between the protected computers and the browser module, and between the protected computers and the unprotected network.

28. (New) The system of claim 21, wherein said browser module is sacrificial and protects the protected computers from unauthorized content.

29. (New) The system of claim 21, wherein said browser isolator module performs detailed field checks and reduce the chance of defect in the protocol implementation on either the browser module or the protected computer.

30. (New) A method for providing a browser interface system for protecting a computer network, said method comprising:

providing communications access to an unprotected network from a protected network via a browser module, wherein the browser module is separate and physically distinct from protected computers;

communicating with the browser module through a browser client module, wherein said browser client module provides control of video and audio output of a browser operating remotely on said browser module;

analyzing communications between the browser module and the browser client module via a browser isolator module; and

preventing unauthorized communications between the browser module and the browser client module via the browser isolator module.

31. (New) The method of claim 30, further comprising limiting the communication between the browser and browser client module to those communications specifically necessary for remote operation of the browser module.

32. (New) The method of claim 31, further comprising screening at least one of the following types of information to determine if the communication is authorized:

source and destination ports, user information, origination information, host information, destination information, character information, IP address information, display identification, session information, display class, display number, TCP information, and date and/or time information.

33. (New) The method of claim 30, said browser module further comprising a distributed network browser.

34. (New) The method of claim 30, further comprising isolating the protected network from unauthorized communications received from the unprotected network.

35. (New) The method of claim 30, further comprising operating any browser-executed code on the browser module.

36. (New) The method of claim 30, said browser isolator module preventing the transfer of permanently stored data between the protected computers and the browser module, and between the protected computers and the unprotected network.

37. (New) The method of claim 30, further comprising protecting the protected computer from unauthorized content, wherein said browser module is sacrificial.

38. (New) The method of claim 30, said browser isolator module performing detailed field checks, said field checks reducing the chance of defect in the protocol implementation on either the browser module or protected computer.

39. (New) A computer program product for providing a browser interface system for protecting a computer network, and including one or more computer-readable instructions embedded on a computer readable medium and configured to cause one or more computer processors to perform the steps of:

providing communications access to an unprotected network from a protected network via a browser module, wherein the browser module is separate and physically distinct from protected computers;

communicating with the browser module through a browser client module, wherein said browser client module provides control of video and audio output of a browser operating remotely on said browser module;

analyzing communications between the browser module and the browser client module via a browser isolator module; and

preventing unauthorized communications between the browser module and the browser client module via the browser isolator module.

40. (New) The computer program product of claim 39, comprising further instructions embedded on the computer readable medium and configured to cause the one or more computer processors to perform the step of limiting the communication between the browser and browser client module to those communications specifically necessary for remote operation of the browser module.

41. (New) The computer program product of claim 40, comprising further instructions embedded on the computer readable medium and configured to cause the one or more computer processors to perform the step of screening at least one of the following types of information to determine if the communication is authorized:

source and destination ports, user information, origination information, host information, destination information, character information, IP address information, display identification, session information, display class, display number, TCP information, and date and/or time information.

42. (New) The computer program product of claim 39, comprising further instructions embedded on the computer readable medium and configured to cause the one or more computer processors to perform the step of said browser module further comprising a distributed network browser.

43. (New) The computer program product of claim 39, comprising further instructions embedded on the computer readable medium and configured to cause the one or more computer processors to perform the step of isolating the protected network from unauthorized communications received from the unprotected network.

44. (New) The computer program product of claim 39, comprising further instructions embedded on the computer readable medium and configured to cause the one or more computer processors to perform the step of operating any browser-executed code on the browser module.

45. (New) The computer program product of claim 39, comprising further instructions embedded on the computer readable medium and configured to cause the one or more computer processors to perform the step of preventing the transfer of permanently stored data between the protected computers and the browser module, and between the protected computers and the unprotected network.

46. (New) The computer program product of claim 39, comprising further instructions embedded on the computer readable medium and configured to cause the one or more computer processors to perform the step of protecting the protected computer from unauthorized content, wherein said browser module is sacrificial.

47. (New) The computer program product of claim 39, comprising further instructions embedded on the computer readable medium and configured to cause the one or more computer processors to perform the step of performing detailed field checks, said field checks reducing the chance of defect in the protocol implementation on either the browser module or protected computer.